US-CERT

UNITED STATES COMPUTER EMERGENCY READINESS TEAM

Monthly Activity Summary
- September 2009 -

This report summarizes general activity as well as updates made to the National Cyber Alert System for September 2009. This includes current activity updates, technical and non-technical cyber security alerts, cyber security bulletins, and cyber security tips, in addition to other newsworthy events or highlights.

Executive Summary

During September 2009, US-CERT issued 18 Current Activity entries, one (1) Technical Cyber Security Alerts, one (1) Cyber Security Alerts, four (4) weekly Cyber Security Bulletins, and two (2) Cyber Security Tips.

Highlights for this month include multiple updates released by Adobe, Apple, Cisco, Microsoft, and Mozilla. Increased activity was observed regarding the Zeus Trojan and fake antivirus phishing campaigns.

Contents

Executive Summary ***1***

Current Activity ***1***

Technical Cyber Security Alerts ***3***

Cyber Security Alerts ***3***

Cyber Security Bulletins ***3***

Cyber Security Tips ***4***

Security Highlights ***4***

Contacting US-CERT ***5***

Current Activity

Current Activity entries are high-impact security threats and vulnerabilities currently being reported to US-CERT. The most significant entries of the month are highlighted below, followed by a table listing all of the entries posted this month.

Current Activity for September 2009	
September 2	Microsoft Internet Information Services (IIS) FTP Service Vulnerability
September 3	Microsoft Releases Advance Notification for September Security Bulletin
September 4	Apple Releases Java Updates for Mac OS X 10.5
September 4	Adobe Flash Vulnerability Affecting Apple Snow Leopard
September 8	Microsoft Releases September Security Bulletin
September 9	Microsoft Releases Security Advisory 975497
September 9	Cisco Releases Security Advisory for a Vulnerability in Multiple Cisco Products

Current Activity for September 2009	
September 10	Apple Releases Security Updates
September 10	Mozilla Releases Security Advisory
September 11	Fraudulent 9/11 Web Sites
September 11	Apple Releases Security Update 2009-005 and Mac OS X v10.6.1
September 18	Adobe Releases Security Bulletin for RoboHelp Server 8
September 22	Microsoft Releases Fix It for SMB Vulnerability
September 23	Montgomery County Animal Shelter Search Engine Poisoning Campaign
September 23	Apple Releases iTunes 9.0.1
September 24	Cisco Releases Multiple Security Advisories for IOS Vulnerabilities and Unified Communications Manager
September 28	Malicious Code Spreading via IRS Scam
September 28	Microsoft Releases Fix It for SMB Vulnerability

- Microsoft released multiple updates in September:
  - A vulnerability affecting the Microsoft Internet Information Services (IIS) FTP service may allow a remote attacker to execute arbitrary code. Additional information regarding this vulnerability can be found in US-CERT Vulnerability Note VU#276653 and Microsoft Security Advisory 975191.
  - Microsoft Security Bulletin Summary for September 2009 addressed multiple Windows vulnerabilities, including the JScript Scripting Engine, Wireless LAN AutoConfig Service, Windows Media Format, Windows TCP/IP, and the DHTML Editing Component ActiveX Control.
  - Microsoft security advisory 975497 and Knowledge Base Article 975497 addressed a vulnerability in Microsoft Server Message Block that could allow an attacker to execute arbitrary code or cause a denial-of-service condition. Exploit code for this vulnerability has been made publicly available as part of the Metasploit Framework.
- Apple released updates for Java, iTunes, iPhone, iPod Touch, and Quicktime.
  - Apple released Java for Mac OS X 10.5 Update 5 to address multiple vulnerabilities in Java, as described in Apple article HT3851. Exploitation of these vulnerabilities may allow an attacker to execute arbitrary code or cause a denial-of-service condition.
  - Security updates iPhone OS 3.1, iPod Touch OS 3.1.1, and Quicktime 7.6.4 addressed vulnerabilities that may allow an attacker to execute arbitrary code, cause a denial-of-service condition, access the system with escalated privileges, or obtain sensitive information. Additional details are described in Apple updates HT3860 and HT3661.
  - Apple has released Security Update 2009-005 and Mac OS X v10.6.1 to address multiple vulnerabilities in a number of applications. These vulnerabilities may allow an attacker to execute arbitrary code, cause a denial-of-service condition, obtain elevated privileges, or access local files. Apple articles HT3865 and HT3864 address the vulnerability previously reported in the "Adobe Flash Vulnerability Affecting Apple Snow Leopard" Current Activity entry.

- Adobe released security bulletin APSB09-14 to address a vulnerability in RoboHelp Sever 8. This vulnerability may allow a remote attacker to execute arbitrary code.
- Cisco has released multiple security advisories during September.
    - Security Advisory cisco-sa-20090908-tcp24 addressed a vulnerability that may allow a remote attacker to cause a denial-of-service condition. This affects Cisco IOS Software, Cisco IOS-XE Software, Cisco CatOS Software, Cisco Adaptive Security Appliance and Cisco PIX, Cisco NX-OS Software.
    - Multiple security advisories were later released to address vulnerabilities in IOS Software and Unified Communications Manager. These vulnerabilities may allow an attacker to cause a denial-of-service condition, buffer overflow, or access control list bypass. Refer to the Cisco Security Advisories dated September 23, 2009. http://www.cisco.com/en/US/products/products_security_advisories_listing.html
- Mozilla has released a security advisories 2009-47, 2009-48, 2009-49, 2009-50, and 2009-51 to address multiple vulnerabilities that may allow an attacker to execute arbitrary code, mislead users by spoofing a URL, or cause a denial of service. These security advisories apply to Firefox.

Technical Cyber Security Alerts

Technical Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits.

Technical Cyber Security Alerts for September 2009	
September 8	TA09-251A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Alerts

Cyber Security Alerts are distributed to provide timely information about current security issues, vulnerabilities, and exploits. They outline the steps and actions that non-technical home and corporate users can take to protect themselves.

Cyber Security Alerts (non-technical) for September 2009	
September 8	SA09-251A Microsoft Updates for Multiple Vulnerabilities

Cyber Security Bulletins

Cyber Security Bulletins are issued weekly and provide a summary of new vulnerabilities recorded by the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD). The NVD is sponsored by the Department of Homeland Security (DHS) National Cyber Security Division (NCSD) / United States Computer Emergency Readiness Team (US-CERT). For modified or updated entries, please visit the NVD, which contains historical vulnerability information.

Security Bulletins for September 2009
SB09-251 Vulnerability Summary for the Week of August 31, 2009
SB09-257 Vulnerability Summary for the Week of September 7, 2009
SB09-264 Vulnerability Summary for the Week of September 14, 2009
SB09-271 Vulnerability Summary for the Week of September 21, 2009

A total of 576 vulnerabilities were recorded in the NVD during September 2009.

Cyber Security Tips

Cyber Security Tips are primarily intended for non-technical computer users and are issued monthly. The September tips focused on email attachments, instant messaging and chat rooms. A link to the full version of this document is listed below.

Cyber Security Tips for September 2009	
September 11	ST04-010 Using Caution with Email Attachments
September 23	ST04-011 Using Instant Messaging and Chat Rooms Safely

Security Highlights

Phishing and Malware Campaigns

Increased activity involving the Zeus Trojan and fake antivirus software was observed during September. Malicious activity continues to be disguised using current events or legitimate organizations:

Malicious Code Spreading via IRS Scam

Public reports of malicious code circulated via spam email messages related to the IRS. The attacks arrive via an unsolicited email message and may contain a subject line of "Notice of Underreported Income." These messages may contain a link or attachment. If users click on this link or open the attachment, they may be infected with malicious code, including the Zeus Trojan. Review the document *How to Report and Identify Phishing, E-mail Scams and Bogus IRS Web Sites* on the IRS website.

Fraudulent 9/11 Web Sites

Public reports indicated that attackers were using legitimate web pages to run malicious code on victims' machines. Reports, including a posting by Sophos, indicate these messages:

- Include keywords and names related to the 9/11/2001 terrorist attack
- Prompt users with a fake virus scan that attempts to make users believe they have a security issue. The users are then asked to download fake security software that is actually malicious code.
- Please note that these characteristics may change at any time.

Montgomery County Animal Shelter Search Engine Poisoning Campaign
Public reports arose regarding a search engine result poisoning campaign affecting search results for the Montgomery County Animal Shelter. Users seeking details on rumors about the closure of a "Montgomery County Animal Shelter" could have been led to click on illegitimate search results, which attempted to download malicious code. The rumors were being spread via e-mail, forums, and social networking sites, usually taking the form of a plea for readers to contact the shelter and adopt animals prior to the shelter's closing.

Recommendations
To mitigate against phishing and other social engineering threats, US-CERT recommends the following steps:

- Do not follow unsolicited web links or attachments in email messages.
- Maintain up-to-date antivirus software.
- Refer to the Recognizing and Avoiding Email Scams (PDF) document for more information on avoiding email scams.
- Refer to the Avoiding Social Engineering and Phishing Attacks document for more information on social engineering attacks.

Contacting US-CERT

If you would like to contact US-CERT to ask a question, submit an incident, or to learn more about cyber security, please use one of the methods listed below. If you would like to provide feedback on this report, or if you have comments or suggestions for future reports, please email info@us-cert.gov.

Web Site Address: http://www.us-cert.gov
Email Address: info@us-cert.gov
Phone Number: +1 (888) 282-0870
PGP Key ID: 0xCB0CBD6E
PGP Key Fingerprint: 2A10 30D4 3083 2D28 032F 6DE3 3D60 3D81 CB0C BD6E
PGP Key: https://www.us-cert.gov/pgp/info.asc